

WHAT IS CLAIMED IS:

1. A method of downloading encrypted e-content to a terminal device comprises:
 - receiving a request for encrypted content from a terminal device;
 - generating a symmetric key and encrypting the e-content with the symmetric key;
 - sending a request to a key server to look up the terminal device public key in a key repository;
 - receiving from the key server the symmetric key encrypted with the public key of the terminal device;
 - generating a unique license ID and producing a new entry in a license repository; and
 - sending a response to the terminal device including the content encrypted with the symmetric key.
2. The method of claim 1 further comprising:
 - activating the license to allow the terminal device to allow consumption of the e-content at the terminal device.
3. The method of claim 1 wherein the request received by the content server comprises:
 - a unique request ID, unique content ID and unique device ID.
4. The method of claim 1 wherein sending the request to the key server comprises:
 - sending a request that includes a unique request ID2, a unique ID of device, and the symmetric key over a secure channel.
5. The method of claim 1 wherein receiving from the key server further includes the unique request ID2, the unique ID of device and the symmetric key encrypted with public key.

6. The method of claim 1 wherein the public key is used for encrypting the symmetric key.

7. The method of claim 1 wherein generating a unique license ID further comprises:

generating a unique license ID and producing a new entry in the license repository and storing the license ID and symmetric key in the license repository.

8. The method of claim 1 further comprising:

receiving a request to register the license with the content server upon receipt of the response to the terminal device from the content server.

9. The method of claim 1 assigning an owner after the license is registered.

10. The method of claim 1 further comprising:

sending from the content server to the key server a free form data to be encrypted with the terminal device's private key to control further properties of content usage; and

receiving by the content server from the key server the encrypted data structure.

11. The method of claim 10 wherein the data structure controls usage characteristics such as expiration date and maximal view count.

12. A method of activating e-content license with terminal device comprises:

sending to a content server a transfer ticket and challenge;

receiving a solved challenge and transfer ticket back from the content server; and

checking the challenge and transfer ticket to activate the e-content license.

13. The method of claim 12 further comprises:

storing the activated e-content license in a protected memory area of the terminal device.

14. The method of claim 12 further comprises:

producing the transfer ticket and the challenge by the terminal device.

15. The method of claim 12 wherein the e-content can be read after completion of activating the license.

16. The method of claim 12 wherein the transfer ticket is used to ensure that registering of e-content licenses happens only once.

17. The method of claim 12 wherein the solved random challenge received from the content server ensures that the terminal device actually communicated with the content server.

18. The method of claim 12 further comprising:

checking, upon receipt of the transfer ticket and the challenge by content server, if the counter value of the transfer ticket matches the expected value of the counter; and incrementing the expected value after checking the counter value.

19. The method of claim 12 wherein the transfer ticket further comprises: a unique counter value, a license id, and device id and wherein the transfer ticket is encrypted with a private key of the terminal device

20. The method of claim 12 wherein the challenge is a random number encrypted with the public key of the terminal device.

21. The method of claim 13 wherein activating the license comprises: setting a flag in the license table in an atomic operation that also increments an internal that tracks the value of the transfer ticket so that it cannot be used again to activate the same license.

22. A method of trading e-content licenses between users, comprises:
unregistering e-content license at a giver's device;
issuing a relinquishing ticket by the giver's device; and
registering the license with a borrower's device using the issued relinquishing ticket.

23. The method of claim 22 wherein issuing a relinquishing ticket by giver's device further comprises:
producing the relinquishing ticket by the giver's device having a counter value, license id and device id; and
encrypting the relinquishing ticket with the private key of the giver's device.

24. The method of claim 23 further comprising:
incrementing the internal relinquishing ticket counter when the license is unregistered.

25. The method of claim 23 further comprising:
producing a copy of the e-content for a giver to transfer to a borrower.

26. The method of claim 23 further comprises:
sending a copy of the relinquishing ticket from the giver device to the borrower device.

27. The method of claim 23 further comprises:
sending the relinquishing ticket to the content server by the giver or the borrower.

28. The method of claim 22 wherein registering comprises:
producing a transfer ticket and challenge and sending the transfer ticket and challenge to the content server.

29. The method of claim 28 wherein upon activation of the license the method further comprises:

receiving from the server a solved challenge, transfer ticket and a license key encrypted with the new device's private key.

30. A method executed on a content server for allowing activation of an e-content license transferred from a giver's terminal device to a borrower's terminal device comprises:
receiving a relinquishing ticket and challenge from the giver's terminal device;
checking a value of the relinquishing ticket;
incrementing the expected value of relinquishing ticket for the giver's device.
assigning borrower device as new owner;
sending a solved challenge and a transfer ticket back to the borrower's terminal device to allow the borrower terminal device to check the challenge and the transfer ticket to activate the e-content license.

31. The method of claim 30 wherein the content server checking the relinquishing ticket further comprises:

decrypting the relinquishing ticket with the public key of the giver's device.

32. The method of claim 30 further comprising:

checking if the relinquishing ticket counter value matches the expected value of the relinquishing ticket and incrementing the expected value thereafter.

33. The method of claim 30 wherein checking the transfer ticket further comprises:

decrypting relinquishing ticket with public key of borrower.

34. The method of claim 30 further comprising:

checking if the transfer ticket's counter matches the expected value of the transfer ticket, and incrementing the expected value thereafter.

35. A method executed on a terminal device for reregistering an e-content licenses after unregistering the e-content, comprises:

 sending by a transfer ticket and a challenge to a content server;

 receiving from the server to the terminal device a solved challenge and checked transfer ticket; and

 checking by the terminal device that the challenge is correct and transfer ticket is correct to activate the e-content license on the terminal device.

36. A method of viewing secure content on a personal computer that executes a non secure operation system, comprises:

 providing a secure extensible computing environment on a personal computer peripheral card; and

 processing the content in an encrypted form in the computer and delivering the content in encrypted form to the secure extensible computing environment on the personal computer peripheral card; and

 decrypting the content in encrypted form on the personal computer peripheral card.